Amendments to the Specification

Please amend the paragraph that begins on page 3, line 8, as follows:

In view of the foregoing, the present invention provides a method and system for a policy agent of a network to authenticate a user that uses a client computer on the network to transmit network communication data[[,]] and to associate the data stream from the client computer with the user. When the client computer initiates a network data connection to or through the policy agent, the policy agent detects the data connection and sends a challenge to the client computer. The challenge is encrypted with a private key of the policy agent. When the client computer ~~received~~ receives the challenge, it decrypts the challenge with the public key of the policy agent and prepares a message digest value, such as by a hash algorithm, based on the data in the challenge and the network data sent by the user. The message digest value is then encrypted with the private key of the user and sent to the policy agent. The policy agent decrypts the received response with the public key of the user to obtain the message digest value. The policy agent then calculates a digest value based on the challenge and the network data received from the client computer[[,]] and compares the calculated digest value with the digest value decrypted from the response. If the two digest values match, the policy agent knows that the user has been authenticated[[,]] and that the received network data are those sent by the user. The policy agent may then apply network policies based on the credentials of the authenticated user.

Please amend the paragraph that begins on page 11, line 1, as follows:

Moreover, the authentication process is independent of the particular network protocol used for transmitting the network data. In accordance with a feature of the invention, the user authentication is performed ~~out-of-band~~ out-of-band, i.e., the network communications for the authentication process are not part of network data stream on which the network policies are to be applied. Few network protocols commonly used for network data transmission have provisions for inclusion of user authentication information as part of the data stream. If an in-band user authentication is to be implemented, those network protocols would have to be substantially modified or entirely replaced with new protocols. Such a solution, however, may not be practical or desirable. The out-of-band user authentication in accordance with the invention avoids the need to include user authentication information in the network data stream on which access policies are to be applied. As a result, the authentication process is independent of the underlying network protocol used to send the data stream and can be used with existing network protocols. With out-of-band user authentication, however, there is a risk that the user

information may be altered or incorrectly associated with the network data stream. As will be described in greater detail below, ~~the~~ user authentication according to the invention effectively avoids this risk by including data from the network data stream in the digital signature process used in the user authentication.

Please amend the paragraph that begins on page 13, line 4, as follows:

After the policy agent has obtained the purported identity of the user associated with the network connection, it obtains a public key of the user (step 106). This may be done, for example, by querying a registry 86 ~~(FIG. 1)~~ (FIG. 2) that maintains a file of public keys of users registered with it. The registry 86 may be separate or the same as the directory server 84. The policy agent then constructs a challenge 90 that is encrypted with its own private key (step 108). The challenge 90 is sent to the client computer 72 (step 110).